CENTRE FOR JOINT WARFARE STUDIES

Aligned with the Future
Victory through Joint Knowledge

SYNODOS PAPER | VOL - XII NO-7 / JUN 2018

ARTIFICIAL INTELLIGENCE (AI) AND ITS APPLICATIONS FOR DEFENCE AND SECURITY FORCES

Air Cmde T Chand (Retd) is a senior Fellow, CENJOW. He is the editor of the Defence Synergy Journal also.

Among the newer generation technological developments, AI, Quantum Computing and Big Data Analytics hold greater promise for the applications in the Defence and Security Forces. These largely Computer Science based technologies are inspired by the relentless research undertaken in the US followed equally seriously in China, Europe, Japan, Russia and Israel. India has also made modest efforts and a Bengaluru based DRDO Laboratory, Centre for Artificial Intelligence and Robotics (CAIR) has developed several technologies for applications in Defence Forces. AI has the potential to revolutionise the way future wars would be fought.

Artificial Intelligence (AI) Simplified

AI is an umbrella term for smart technologies that are aware of and can learn from their environments, enabling them to subsequently take autonomous action. Robotic process automation, machine learning, natural language processing, and neural networks all incorporate AI into their operations. AI is different from general purpose software as it enables machines to respond autonomously to inputs from the external world, inputs that programmers do not directly control and therefore cannot always anticipate[1]. In broad definition, AI is a collective term for computer systems that can sense their environment, think, learn, and take action in response to what they are sensing. Forms of AI in use today include, among others; digital assistants, chat bots and machine learning. AI works in four ways, namely, automated intelligence which deals with the automation of manual or cognitive and routine or non-routine tasks; assisted intelligence which helps people to perform tasks faster and better; augmented intelligence which helps people to make better decisions and autonomous intelligence which leads to automating decision making processes without human intervention.[2] A brief description of a few technical terms usually employed in AI literature often leads to a better understanding of its potential applications.

Technical Aspects of the AI

In an article titled "Some specific tech aspects of Artificial Intelligence", André M. König, has described various technical terms used in the discussion on AI.[3] There are two vastly differing approaches to AI namely: general and narrow AI also called strong and weak AI. Strong AI is a hypothetical machine that exhibits behaviour at least as skilful and flexible as humans do, and the research programme of building such an artificial general intelligence. It is in its infant stage, but is likely to develop faster due to recent developments in nanotechnology. A strong AI builds its own models based on raw input. The principle behind Strong AI is that the machines could be made to think or could represent human minds in the future. Those machines will have the ability to reason, think and do all functions that a human is capable of doing. Weak AI on the other hand uses models of its problem domain given to it by programmers. The principle behind Weak AI is simply the fact that machines can be made to act as if they are intelligent like a computer playing the chess with a human player on the basis of pre programmed moves by the humans.

Machine Learning. Machine learning is the practice of using algorithms to parse data, learn from it, and then make a determination or prediction about something pertaining to the data. So, rather than hand-coding software routines with a specific set of instructions

[1] Chris Curran and Anand Rao; PWC Briefing: Artificial intelligence; http://usblogs.pwc.com/emerging-technology/briefing-ai/

[2] Chris Curran and Anand Rao; PWC Briefing: Artificial intelligence; http://usblogs.pwc.com/emerging-technology/briefing-ai/

[3] Andre M Konig, "Some specific tech aspects of Artificial Intelligence"; https://www.linkedin.com/pulse/some-specific-tech-aspects-artificial-intelligence-andr%C3%A9-m-k%C3%B6nig

to accomplish a particular task, the machine is trained using large amounts of data and algorithms that give it the ability to learn how to perform the task. One of the very best application areas for machine learning for many years was computer vision, though it still required a great deal of hand-coding to get the job done. Machine learning is closely associated with the deep learning.

Deep Learning. Deep learning is a branch of machine learning based on a set of algorithms that attempt to model high level abstractions in data. In a simple case, you could have two sets of neurons: ones that receive an input signal and ones that send an output signal. When the input layer receives an input it passes on a modified version of the input to the next layer. In a deep network, there are many layers between the input and output, allowing the algorithm to use multiple processing layers, composed of multiple linear and non-linear transformations. Deep learning is part of a broader family of machine learning methods based on learning representations of data. Both machine learning and deep learning bank heavily on data science outcomes.

Data Science. It is an interdisciplinary field about scientific processes and systems to extract knowledge or insights from data in various forms, either structured or unstructured, which is a continuation of some of the data analysis fields such as statistics, machine learning, data mining, and predictive analytics. Jim Gray imagined data science as a fourth paradigm of science (empirical, theoretical, computational and now data-driven) and asserted that everything about science is changing because of the impact of information technology and the data deluge. Data science employs techniques and theories drawn from many fields within the broad areas of mathematics, statistics, operations research, information science, and computer science, including signal processing, probability models, machine learning, statistical learning, data mining, data engineering, pattern recognition and learning, predictive analytics, uncertainty modeling, data warehousing, data compression, artificial intelligence, and high performance computing. The development of machine learning has enhanced the growth and importance of data science. Data science affects academic and applied research in many domains, including machine translation, speech recognition, robotics, search engines, digital economy, biological sciences, medical informatics, health care, social sciences and the humanities. It heavily influences economics, business and finance. From the business perspective, data science is an integral part of competitive intelligence, a newly emerging field that encompasses a number of activities, such as data mining, data analysis and predictive analytics.

Predictive Analytics. It encompasses a variety of statistical techniques from predictive modeling, machine learning, and data mining that analyse current and historical facts to make predictions about unknown events. In business, predictive models exploit patterns found in historical and transactional data to identify risks and opportunities. Models capture relationships among many factors to allow assessment of risk or potential associated with a particular set of conditions, guiding decision making for candidate transactions. The defining functional effect of these technical approaches is that predictive analytics provides a predictive score i.e. probability for each individual such as customer, employee, healthcare patient, vehicle, component, machine, or other organisational unit in order to determine, inform, or influence organisational processes that pertain across large numbers of individuals, such as in marketing, credit risk assessment, fraud detection, manufacturing, healthcare, and government operations including law enforcement.

Natural Language Processing (NLP). Natural language processing is a field of computer science, artificial intelligence, and computational linguistics, concerned with the interactions between computers and human languages. As such, NLP is related to the area of human–computer interaction. Modern NLP algorithms are based on machine learning, especially statistical machine learning. Emerging trends in the fast developments of AI technologies indicate their possible applications in the defence and security forces related systems in the future.

AI Development Trends

Messrs Rao, Voyles and Ramchandani have listed a few emerging AI trends in their paper on this subject and have been summarised in the following paragraphs.[4] These trends also indicate their likely future applications.

Deep Neural Networks, which mimic the human brain, have demonstrated their ability to learn from image, audio, and text data suggesting that after an initial fitting phase, a deep neural network will forget and compress noisy data; that is, data sets containing a lot of additional meaningless information, while still preserving information about what the data represents. It can yield insights into optimal network design and architecture choices, while providing increased transparency for safety-critical or regulatory applications.

Capsule Networks, a new type of deep neural network, process visual information in much the same way as the brain, which means they can maintain hierarchical relationships. This is in stark contrast to convolutional neural

[4] Anand Rao, Joseph Voyles and Pia Ramchandani; Top 10 artificial intelligence (AI) technology trends for 2018; http://usblogs.pwc.com/emerging-technology/top-10-ai-tech-trends-for-2018/

networks, one of the most widely used neural networks, which fail to take into account important spatial hierarchies between simple and complex objects, resulting in misclassification and a high error rate.

Deep Reinforcement Learning (DRL) involves interacting with the environment to solve business problems. DRL has been used to learn gaming strategies, such as Atari and Go, including the famous Alpha Go programme that beat a human champion. DRL is the most general purpose of all learning techniques, so it can be used in the most business applications. It also requires less data than other techniques to train its models. It can be trained via simulation, which eliminates the need for labeled data entirely.

A Generative Adversarial Network (GAN) is a type of unsupervised deep learning system that is implemented as two competing neural networks. One network, the generator, creates fake data that looks exactly like the real data set. The second network, the discriminator, ingests real and synthetic data. Over time, each network improves, enabling the pair to learn the entire distribution of the given data set. GANs open up deep learning to a larger range of unsupervised tasks in which labeled data does not exist or is too expensive to obtain. They also reduce the load required for a deep neural network because the two networks share the burden. It is likely to be employed in cyber detection applications in future.

Probabilistic Programming is a high-level programming language that more easily enables a developer to design probability models and then automatically solve these models. Probabilistic programming languages make it possible to reuse model libraries, support interactive modeling and formal verification, and provide the abstraction layer necessary to foster generic, efficient inference in universal model classes. Probabilistic programming languages have the ability to accommodate the uncertain and incomplete information that is so common in the business domain. These languages are expected to be applied to deep learning.

Hybrid Learning Models. Different types of deep neural networks, such as GANs or DRL, have shown great promise in terms of their performance and widespread application with different types of data. However, deep learning models do not model uncertainty, the way Bayesian, or probabilistic, approaches do. Hybrid learning models combine the two approaches to leverage the strengths of each. Some examples of hybrid models are Bayesian deep learning, Bayesian GANs, and Bayesian conditional GANs. Hybrid learning models make it possible to expand the variety of business problems to include deep learning with uncertainty. This is likely to result in achieving better performance and explainability of models, which in turn could encourage more widespread adoption.

Automated Machine Learning (AutoML). Developing machine learning models requires a time-consuming and expert-driven workflow, which includes data preparation, feature selection, model or technique selection, training, and tuning. AutoML aims to automate this workflow using a number of different statistical and deep learning techniques. AutoML is part of democratisation of AI tools, enabling business users to develop machine learning models without a deep programming background. It will also speed up the time it takes data scientists to create models.

A Digital Twin is a virtual model used to facilitate detailed analysis and monitoring of physical or psychological systems. The concept of the digital twin originated in the industrial world where it has been used widely to analyse and monitor things like windmill farms or industrial systems. Digital twins are being applied to nonphysical objects and processes, including predicting customer behavior. Digital twins can help spur the development and broader adopting of the internet of things (IoT), providing a way to predictively diagnosis and maintain IoT systems.

Explainable AI. Presently, there are scores of machine learning algorithms in use that sense, think, and act in a variety of different applications. Yet many of these algorithms are considered black boxes, offering little insight into how they reached their outcome. Explainable AI is a movement to develop machine learning techniques that produce more explainable models while maintaining prediction accuracy. AI that is explainable, provable, and transparent will be critical to establishing trust in the technology and will encourage wider adoption of machine learning techniques. Enterprises will adopt explainable AI as a requirement or best practice before embarking on widespread deployment of AI, while governments may make explainable AI a regulatory requirement in the future. Globally, many countries have embarked on to various AI programmes both for military and dual use applications.

Global AI Developments (Defence and Security Applications)[5]

Russia. Russia has been working on AI guided missiles that can decide to switch targets mid-flight. Reportedly, there already exists completely autonomous AI operation systems that provide the means for UAV clusters, to fulfill missions autonomously, sharing tasks between them, and interact. Russia believes that it is inevitable that swarms of drones will one day fly over combat zones. Russia has been testing several autonomous and semi-autonomous combat systems,

[5] Artificial intelligence arms race; https://en.wikipedia.org/wiki/Artificial_intelligence_arms_race

such as Kalashnikov's neural net combat module, with a machine gun, a camera, and an AI that possibly can make its own targeting judgments without human intervention. The Russian government has strongly rejected any ban on lethal autonomous weapons systems, suggesting that such a ban could be ignored.

China. China sees itself as close competitor of the United States in AI. The Chinese military intends to achieve an advantage through changing paradigms in warfare with military innovation. The close ties between Silicon Valley and China, and the open nature of the American research community, has made the West's most advanced AI technology easily available to China. Chinese industry has numerous home-grown AI accomplishments of its own, such as Baidu passing a notable Chinese-language speech recognition capability benchmark in 2015. As of 2017, China's roadmap aims to create a $150 billion AI industry by 2030. China often sources sensitive emerging technology such as drones and artificial intelligence from private startup companies. The Japan Times reported in 2018 that annual private Chinese investment in AI is under $7 billion per year. AI startups in China received nearly half of total global investment in AI startups in 2017. Of late, Chinese institutions have filed for nearly five times as many AI patents as did Americans.

USA. US believe that the rapid advances in artificial intelligence will define the next generation of warfare. For 2018 the United States private investment in AI is expected to be around $70 billion. The U.S. has many military AI combat programmes, such as the Sea Hunter autonomous warship, which is designed to operate for extended periods at sea without a single crew member, and to even guide itself in and out of port. As of 2017, a temporary US Department of Defence directive requires a human operator to be kept in the loop when it comes to the taking of human life by autonomous weapons systems.

Israel. Israel has designed a Harpy anti-radar, fire and forget drone is to be launched by ground troops, and autonomously fly over an area to find and destroy radar that fits pre-determined criteria.

AI Developments in India

In an ambitious defence project, the Indian Govt has started work on incorporating AI to enhance the operational preparedness of the armed forces in a significant way that would include equipping them with unmanned tanks, ships, aerial vehicles and robotic weaponry. The move is part of a broader policy initiative to prepare the defence and security forces for next generation warfare. A task force is finalising the specifics and framework of the project, which would be implemented in a partnership model between the armed forces and the private sector[6]. The

[6] https://www.livemint.com/Politics/DklacCY1p9ujhgyE9WjIJP/India-working-on-artificial-intelligence-application-to-boos.html, 20 May 2018

government is banking on this multi-stakeholder taskforce, which was set up in February 2018, to formulate a concrete strategy and framework for employment of AI for national security and defence needs in the years ahead. The 17-member taskforce, which is headed by Tata Sons chairman N Chandrasekaran and includes national cyber security coordinator Gulshan Rai, IIT and IISc professors as well as two and three-star generals and representatives from ISRO, DRDO and Atomic Energy Commission, is working on the roadmap with several goals in mind. They range from establishing tactical deterrence in the region and visualizing potential transformative weaponry to developing intelligent, autonomous robotic systems and bolstering cyber defence. The taskforce will make recommendations on how to make India a significant power in AI, in terms of both offensive and defensive needs, especially in aviation, naval, land systems, cyber, nuclear and biological warfare arenas. Initial tender is likely to be floated over the next two years on dual use AI capabilities. Concurrently, DRDO's CAIR is also trying to develop different kinds of intelligent robots. India, of course, also needs to take cognisance of the entire ethical debate on Lethal Autonomous Weapon Systems (LAWS) because critics argue they could violate humanitarian principles by having the capability to autonomously select and destroy targets without human intervention.

Recommendations of the task force are likely to come in by June 2018. India has a fairly strong IT industry base and that is going to be biggest strength in terms of developing AI capabilities. DRDO would be a major player in the project. There is an enormous potential for the use of AI in the civilian sphere as well and the task force would be also looking into it. It may be noted that the urgency for AI-enhanced defence systems was also highlighted in April 2018 by Indian Prime Minister at the Defence Expo 2018 in Chennai.

Disclaimer: Views expressed are of the author and do not necessarily reflect the views of CENJOWS

CENTRE FOR JOINT WARFARE STUDIES
Kashmir House, Rajaji Marg, New Delhi-110 001
Tel. Nos : 011-23792446, 23006535, 3306538/9, Fax : 011-23792444
Website : http://cenjows.gov.in, e-mail : cenjows@yahoo.com

www.xtremeonline.in # 9811707220